



แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Network and Server Policy)

โรงพยาบาลเกาะกูด กำหนดมาตรฐานความปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server)
ดังนี้

๑. ผู้ดูแลระบบ ต้องแบ่งระบบเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มของผู้ใช้งาน คือ เครือข่ายภายใน (Internal Network) และ เครือข่ายภายนอก (External Network) เพื่อให้สามารถควบคุมป้องกันการบุกรุกได้อย่างเป็นระบบ
๒. หากผู้ใช้บริการ ต้องการนำเครื่องคอมพิวเตอร์ และอุปกรณ์อื่นจากภายนอกมาเชื่อมต่อเข้ากับเครื่องคอมพิวเตอร์และระบบเครือข่ายของหน่วยงาน ต้องได้รับอนุญาตจากผู้อำนวยการโรงพยาบาล หรือหัวหน้ากลุ่มงานประกันสุขภาพ ยุทธศาสตร์ และสารสนเทศทางการแพทย์ก่อน และต้องปฏิบัติตามนโยบายนี้โดยเคร่งครัด
๓. ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้ง เพิ่มเติม หรือทำการใดๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลัก โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ
๔. ผู้ดูแลระบบต้องควบคุมการเข้าถึงระบบเครือข่าย เพื่อบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพ ดังต่อไปนี้
 - ๔.๑ กำหนดให้มีการจำกัดสิทธิ์การใช้งาน เพื่อควบคุมผู้ใช้บริการให้สามารถใช้งานเฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น
 - ๔.๒ กำหนดให้มีการจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังคอมพิวเตอร์แม่ข่าย
 - ๔.๓ ระบบเครือข่ายทั้งหมดของหน่วยงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอกหน่วยงานต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก รวมทั้งต้องมีความสามารถในการตรวจจับโปรแกรมประสงค์ร้าย (Malware) ด้วย
 - ๔.๔ ระบบเครือข่ายต้องติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention System / Intrusion Detection System) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งาน ระบบเครือข่ายของหน่วยงานในลักษณะที่ผิดปกติ
 - ๔.๕ การเข้าสู่ระบบเครือข่ายภายในหน่วยงาน โดยผ่านทางระบบอินเทอร์เน็ตจำเป็นต้องมีการลงบันทึกเข้า (Login) และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้องของผู้ใช้บริการ
 - ๔.๖ เลขที่อยู่ไอพี (IP Address) ภายในของระบบเครือข่ายในของหน่วยงานจำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้
 - ๔.๗ จัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับของเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๔.๘ การใช้เครื่องมือต่างๆเพื่อการตรวจสอบระบบเครือข่าย ต้องได้รับการอนุญาตจากผู้ดูแลระบบ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

๔.๙ ผู้ดูแลระบบต้องบริหารควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) และรับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย ในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่างๆของซอฟต์แวร์ระบบ (System Software)

๕. โรงพยาบาลเกาะกูด กำหนดมาตรฐานการควบคุมการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์ (Log) มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ตามแนวทาง ดังต่อไปนี้

๕.๑ กำหนดให้มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน Command Line และ Firewall Log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย ๙๐ วัน นับตั้งแต่การใช้บริการสิ้นสุดลง

๕.๒ ตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานระบบอย่างสม่ำเสมอ

๕.๓ จำกัดสิทธิ์การเข้าถึงบันทึกให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

๖. โรงพยาบาลเกาะกูด กำหนดมาตรฐานการควบคุมการใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอกตามแนวทาง ดังต่อไปนี้

๖.๑ บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายของหน่วยงาน ต้องทำหนังสือขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุญาตจากผู้อำนวยการโรงพยาบาล หรือหัวหน้ากลุ่มงานประกันสุขภาพ ยุทธศาสตร์ และสารสนเทศทางการแพทย์

๖.๒ มีการควบคุมช่องทางที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

๖.๓ วิธีการใดๆที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้จากกระยะไกลต้องได้รับการอนุญาตจากผู้อำนวยการโรงพยาบาล หรือหัวหน้ากลุ่มงานประกันสุขภาพ ยุทธศาสตร์ และสารสนเทศทางการแพทย์

๖.๔ ตลอดระยะเวลาที่ใช้งาน เจ้าหน้าที่ที่เกี่ยวข้องจะต้องประจำอยู่ที่หน้า และบันทึกหน้าจอการทำงานทุกครั้ง

๖.๕ การเข้าสู่ระบบจากกระยะไกล ผู้ใช้งานต้องแสดงหลักฐาน ระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับหน่วยงานอย่างเพียงพอ

ประกาศ ณ วันที่ ๑๖ มีนาคม พ.ศ. ๒๕๖๖

(นายณัฐภัทร ศรีอุดมพร)
นายแพทย์ปฏิบัติการ รักษาการในตำแหน่ง
ผู้อำนวยการโรงพยาบาลเกาะกูด